

AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

- 1 1. (Currently Amended) A method for predicting potential points-of-compromise, the
2 method comprising:
3 storing a database correlating each first member of a first set, wherein each of said first
4 members may be compromised ~~in time~~, with each second member of a second set, wherein each
5 of said second members may be a potential point-of compromise;
6 recording in said database each interaction of a first member with a second member;
7 ~~[[from]]~~ for a given third set of third members, wherein each of said third members is a
8 given compromised first member~~[[,]]~~ from said database, selecting ~~each interaction~~ interactions
9 associating said third members and said second members;
10 calculating ~~[[an]] interaction factor for each of said third members from each said~~
11 interaction factors for respective second members that are part of interactions involving the third
12 members, each interaction factor indicating a number of occurrences of interactions involving
13 said third members at a corresponding second member; and
14 predicting at least one potential point-of-compromise from results of said calculating.
- 1 2. (Original) The method as set forth in claim 1 said selecting further comprising:
2 for each of said third members, including each said interaction found for a predetermined
3 past time period.
- 1 3. (Currently Amended) The method as set forth in claim 2 wherein each said
2 predetermined past time period is determined individually from a given ~~time-of-first-know-fraud~~
3 time-of-first-known-fraud for each of said third members.
- 1 4. (Currently Amended) The method as set forth in claim 3 wherein said storing and said
2 recording further comprises:
3 dividing said database into a plurality of separately retrievable files, wherein each of said
4 files is characterized by a predetermined time frame bounding interactions between said first
5 members and said second members.

1 5. (Currently Amended) The method as set forth in claim 4 wherein for each of said third
2 members, ~~[[said]]~~ each said time-of-first-known-fraud and said predetermined past time frame
3 ~~[[is]]~~ are used to filter out those separately retrievable files not within said predetermined past
4 time period from said selecting.

1 6. (Original) The method as set forth in claim 4 wherein said separately retrievable files are
2 created using identifier features of said second members suited to maximizing data compression.

1 7. (Currently Amended) The method as set forth in claim 1, said storing further comprising:
2 segregating correlated first members and second members into a plurality of data files,
3 wherein said files are identifiable via a predetermined common characteristic of at least one
4 predetermined particular characteristic of a selected ~~[[on]]~~ one of said first members ~~[[or]]~~ and
5 said second members.

1 8. (Cancelled)

1 9. (Currently Amended) The method as set forth in claim 1, said predicting further
2 comprising:
3 listing all second members associated in said selecting as a potential point-of-
4 compromise with a score based upon ~~a tally of interactions between said third members and said~~
5 ~~second members~~ the interaction factors.

1 10. (Currently Amended) The method as set forth in claim 9, said predicting further
2 comprising:
3 adjusting each said score by a common factor associated with each said second member
4 ~~associated in said selecting wherein all~~ to normalize the scores are normalized.

1 11. (Currently Amended) A method for identifying possible points-of-compromise, the
2 method comprising:
3 creating a matrix correlating a plurality of at least ~~two identifiers~~ first items and second
4 items, each second item representing a potential point-of-compromise;
5 logging in said matrix every interactivity involving ~~individual ones of pairs~~ [[each]] of
6 said ~~two identifiers~~ first and second items;
7 [[from]] for a given ~~set of first specific identifiers~~ subset of the first items, extracting
8 from said matrix all interactivities ~~with second identifiers for~~ of the first items in said [[set]]
9 subset with second items;
10 tabulating extracted said interactivities according to frequency of said interactivities; and
11 assigning a point-of-compromise score to each of said ~~first identifiers~~ second items that
12 are involved in the extracted interactivities, wherein each said score is indicative of frequency of
13 the extracted interactivities occurring at the corresponding second item.

1 12. (Currently Amended) The method as set forth in claim 11 further comprising:
2 sorting said matrix into a plurality of data files such that in each of said files one of said
3 ~~identifiers~~ first and second items has a predetermined unique characteristic; ~~and~~
4 ~~using a given identifier having said characteristic, retrieving from one of said files~~
5 ~~associated with said characteristic, each second identifier from said matrix having at least one of~~
6 ~~said interactivities.~~

1 13. (Original) The method as set forth in claim 11 further comprising:
2 limiting said extracting to a predetermined past time frame.

1 14. (Currently Amended) The method as set forth in claim 12 wherein each of said files is
2 associated with a common structure or characteristic of at least one of said ~~identifiers~~ first and
3 second items.

1 15. (Currently Amended) The method as set forth in claim 11 wherein each said extracted
2 interactivity is a data pair further comprising a ~~[[fixed]]~~ first identifier representative of a
3 compromised ~~identifier~~ first item and an interactivity situation identifier.

1 16. (Cancelled)

1 17. (Currently Amended) A data storage and data mining process for determining at least
2 one probable point-of-compromise for members of a data set, the process comprising:

3 in a set of data files, logging every individual transaction between first members and
4 second members, wherein said first members are subject to compromise and said second
5 members are each a potential point-of-compromise;

6 ~~[[from]]~~ for a given set of compromised first members, segregating a subset of the data
7 files for a predetermined past time period, ~~[[past]]~~ wherein said subset has at least one of said
8 first members logged therein;

9 for each of said second members in said subset, incrementing a ~~separate~~ corresponding
10 second member tally ~~[[for]]~~ in response to each said individual transaction associated with each
11 one of said compromised first members, and creating a set of the second member tallies that are
12 associated with ~~each of said~~ respective second members; and

13 organizing said set of second member tallies according to a predetermined scoring
14 statistic associated with probability of point-of-compromise.

1 18. (Currently Amended) A data storage and data mining system for determining at least one
2 probable point-of-compromise for members of a data set, the system comprising:

3 means for storing data files;

4 means for logging in said data files every individual transaction between first members
5 and second members, wherein said first members are subject to compromise and said second
6 members are each a potential point-of-compromise;

7 [[from]] for a given set of compromised first members, means for segregating a subset of
8 the data files for a predetermined past time period, [[past]] wherein said subset has at least one of
9 said first members logged therein;

10 for each of said second members in said subset, means for incrementing a ~~separate~~
11 corresponding second member tally [[for]] in response to each said individual transaction
12 associated with each one of said compromised first members and for creating a set of the second
13 member tallies that are associated with ~~each of said~~ respective second members; and

14 means for organizing said set of second member tallies according to a predetermined
15 scoring statistic associated with potential as a point-of-compromise.

1 19. (Currently Amended) A method of determining credit card fraud point-of-compromise
2 scores, the method comprising:

3 correlating [[all]] issued credit cards with [[all]] authorized points-of-use such that ~~every~~
4 ~~transaction~~ transactions involving use of a credit card [[is]] are retrievably logged in a database;

5 [[from]] for a given set of compromised credit cards, extracting from said database all
6 transactions involving use of each of said compromised credit cards;

7 for each of said authorized points-of-use involved in at least one of said transactions
8 involving at least one of said compromised credit [[card]] cards, creating a tally of said
9 transactions for each point-of-use, and incrementing each said tally for each occurrence of
10 transaction involving at least one of said compromised credit cards;

11 sorting said authorized points-of-use ~~having a tally~~ according to ~~tally score~~ the tallies;
12 and

13 assigning a score representative of point-of-compromise likelihood to each of said
14 authorized points-of-use ~~having a tally~~ according to ~~said tally score~~ the respective tally.

1 20. (Original) The method as set forth in claim 19 wherein said extracting is limited to a
2 predetermined time period range of past transactions.

1 21. (Currently Amended) The method as set forth in claim 19 wherein each said [[tally]]
2 score is normalized via a characteristic related to point-of-use.

1 22. (Original) The method as set forth in claim 19 wherein said database comprises a
2 plurality of files wherein each of said files is characterized by a given time frame bounding said
3 transactions logged.

1 23. (Original) The method as set forth in claim 22 wherein each of said plurality of files is
2 sortable by identifier data representative of subsets of credit card numbers.

1 24. (Cancelled)

1 25. (Original) The method as set forth in claim 20 wherein said predetermined time period
2 range of past transactions is based upon a given suspected time-of-compromise window prior to
3 a time-of-first-known-fraud for each said credit card.

1 26. (Original) The method as set forth in claim 22 wherein said files comprise a matrix of
2 data compressed identifier pairs wherein each of said pairs includes a credit card identifier and a
3 point-of-use situation identifier.

1 27. (Currently Amended) The method as set forth in claim 26 ~~wherein~~ further comprising
2 providing a first database ~~comprises~~ comprising a relational data pair relating said point-of-use
3 situation identifier and said credit card identifier, and a second database correlating each said
4 point-of-use situation identifier to a physical said point-of-use.

1 28. (Currently Amended) A method of doing business comprising:

2 receiving a set of credit card numbers and a set of merchants authorized to accept said
3 credit cards;

4 forming a matrix of said numbers and said merchants;

5 logging each use of a card with a merchant as a predetermined data point of said matrix;

6 ~~[[from]]~~ for a given set of compromised credit card numbers, extracting ~~therefor over a~~
7 ~~predetermined given time period,~~ each related said data point of said matrix;

8 incrementing a tally for each merchant associated with each related said data point; and

9 sorting said merchants according to the tallies ~~by tally score; and~~

10 ~~assigning a probability of point-of-compromise for said list of compromised credit card~~
11 ~~numbers based on said tally score.~~

1 29. (Original) A computer memory comprising:

2 computer code for compiling a database wherein members of a first class are associated
3 with members of a second class in accordance with each interaction of a member of the first
4 class with a member of the second class;

5 computer code for extracting from said database only those interactions for a
6 predetermined past time period associated with a given subset of members of the first class

7 wherein said given subset represents individual compromised members of said first class; and

8 computer code for assigning a score to individual members of the second class for each
9 of said interactions extracted wherein said score represents a point-of-compromise probability
10 for each of said individual members of the second class.

1 30. (Currently Amended) Given a computerized matrix of interactivity events between
2 items-of-use, each having a unique first identifier, and points-of-use, each having a unique
3 second identifier, and a set of compromised said items-of-use, wherein said matrix further
4 comprises a plurality of files, each of said files covering a given time frame for said interactivity
5 events, a method for point-of-compromise scoring comprising:
6 determining a time-of-first-known-fraud for each said compromised said items-of-use;
7 for each said compromised said items-of-use, assigning a suspected date window prior to
8 said time-of-first-known-fraud;
9 selecting those ones of said files included in said suspected date window, wherein said
10 compromised said items-of-use are included in said files;
11 for each selected file and for each compromised said items-of-use, counting the number
12 of said interactivity events for each of said points-of-use in each said selected file; and
13 assigning the highest score indicative of point-of-compromise to a highest scoring one of
14 said points-of-use.

1 31. (New) The data storage and mining process of claim 17, wherein incrementing each
2 second member tally comprises incrementing a corresponding count of a number of occurrences
3 of transactions involving the compromised first members at the corresponding second member.

1 32. (New) The data storage and data mining system of claim 18, wherein each second
2 member tally comprises a count of a number of occurrences of transactions involving the third
3 members at the corresponding second member.